Harkia Accountants Limited COMPUTER USE POLICY

INTRODUCTION

Purpose of the policy

The purpose of this policy is to provide clear procedures and guidance for users on the appropriate use of email, intranet and internet facilities on all our computer systems. This policy does not cover all of the obligations of users to comply with data protection law, and it should be read in conjunction with our data protection policy.

Scope of the policy

The policy applies to all employees; fixed-term contract employees; temporary employees; agency staff; and consultants and contractors who are provided with access to any of the Firm's computer systems. Collectively these individuals are referred to as 'users' throughout this policy.

Policy statement

It is our policy to encourage responsible use of email, the intranet and the internet and thus to protect both the Firm and its business, and also all those who work for us. This policy aims to guide users as to the appropriate use of work systems, to preserve the security of the Firm's computer systems, to protect the Firm and its employees against the threat of legal action and to encourage high standards of behaviour and conduct in relation to the use of these communication tools.

We recognise the significant benefits of email, intranet and internet usage and the facilities which are provided represent a considerable commitment of resources for telecommunications, networking, software and storage.

Internet, intranet and email use is provided by the Firm for business-related purposes, ie to communicate with clients, suppliers and colleagues, to research relevant topics and to obtain useful business information. Inappropriate, unnecessary or unauthorised internet, intranet and email has a number of potential implications. It may be used

- to access inappropriate material, or to harass or abuse others
- to undermine the reputation of the Firm and/or those who work for it
- in a way that ties up the Firm's resources unnecessarily and/or has cost implications
- to alter the Firm's legal position without authority
- to waste work time.

General points

Users must not attempt to access information, messages or emails, computer files or computer systems for which they are not authorised and this is likely to constitute a serious disciplinary offence. Unauthorised access to computer networks may also be a criminal offence under the General Data Protection Regulation (GDPR) and the Computer Misuse Act 1990. Users must keep their passwords confidential and rules relating to the security of passwords are contained within the Firm's data protection policy.

No software or files (including but not limited to screensavers, games, bitmaps, backgrounds, gifs and the like) may be downloaded via the internet, intranet or email or installed onto the Firm's network unless authorised by Director. Any file which is downloaded must be scanned for viruses before it is run or accessed. Users must not use or incorporate

any hardware not owned by the Firm into the Firm's computer system without Director's express permission, including external data hard drives or disks.

USE OF EMAIL

Email makes a major contribution to efficient internal and external communication, but it should be used sensibly. The combination of informality and lack of inhibition with email may lead users to regard it as less formal and less important than a formal letter. However, using email inappropriately can result in a user, intentionally or inadvertently

- sending or receiving pirated software or unsuitable material, or publishing defamatory statements
- disclosing the Firm's confidential information
- misleading recipients
- entering into legally binding contractual obligations on behalf of the business without authorisation, changing the Firm's contractual position or otherwise breaching legal obligations
- subjecting users or third parties to harassment or discrimination on the grounds of their sex, race or disability and/or bullying or intimidating colleagues
- making statements which harm the Firm's reputation
- introducing or spreading viruses across the system
- Inappropriately disclosing personal data and/or failing to maintain security of personal data in breach of the GDPR.

To minimise these risks, to protect colleagues, and to maintain the integrity of the Firm's image and reputation, all users should adhere to the following guidance.

Security of email communications

Generally, emails must be [encrypted or otherwise protected within the firm's security system], and this is dealt with in the data protection policy. However, users must be aware that an email message is not necessarily a confidential means of communication. It is an insecure medium and content can be read, and in certain circumstances copied, as well as stored and archived. Therefore it is safer to regard emails as a permanent written record, which may be read by persons other than the addressees.

Confidentiality of email

Users should never send strictly confidential messages or messages containing personal data by email. Users must not expect any email messages composed, received or sent on the Firm's network, regardless of the use of passwords or encryption, to be for private viewing only. Because email passes over the public internet and could be accessed by others, emails sent to any email address outside the business cannot be assumed to be secure. All external emails must have the following disclaimer attached to them; failure to attach the disclaimer is a disciplinary offence:

> *This email and any attachments are confidential. It is intended for the recipient only. If you are not the intended recipient, any use, disclosure, distribution, printing or copying of this email is unauthorised. If you have received this email in error, please immediately notify the sender by replying to this email and delete the email from your computer.*
>
> *The contents of any attachment to this email may contain software viruses, which could damage your own computer system. While we have taken every*

reasonable precaution to minimise this risk, we cannot accept liability for any damage which you sustain as a result of software viruses. You should carry out your own virus checks before opening the attachment.

Content of emails

The use of our email systems for any of the following is strictly prohibited:

- drafting, sending or forwarding any email which might be considered by a recipient to be offensive, defamatory, discriminatory or bullying, eg on the grounds of sex, sexual orientation, age, religion, race or disability or any other personal characteristic

- accessing, circulating, distributing or otherwise publishing offensive material, including pornography; 'offensive' means anything giving or meant or likely to give offence or insult

- entering into a legally binding contract, or making a statement which might later bind the Firm unless users are authorised by their manager to do so

- making any statements which might in the reasonable opinion of the Partners cause harm to the Firm's reputation

- disclosing confidential business information, or disclosure of personal data in breach of the Data Protection Policy

- circulating messages with large attachments – for example, large files, video clips or games, non-standard screen savers/wallpaper or games

- circulating email 'chain letters'.

To minimise the risk of virus infection, users should not open emails from unknown sources or emails which have attachments which look suspicious or are from a source which does not usually send attachments. [person] should be contacted immediately and they will check that the attachment is free from viruses. Users must immediately comply with any instructions given by [person].

Users must not infringe copyright or trademark laws when composing or forwarding emails or email attachments; for example, users should not copy material (such as artwork) created by third parties unless the user has their express permission.

Users must not upload any software onto the Firm's computer system, whether it is licensed to the Firm or not. Any software to be installed on our systems will be dealt with by [person].

Storage of large numbers of emails uses up valuable memory. Where possible, emails which are no longer required should be deleted or archived

Monitoring of email communications

The Firm's email facilities are provided for business use only. Limited personal use of email is acceptable provided it is for occasional social or domestic use only and does not relate to private business activities. Users should be aware that emails are monitored by the Firm, as indicated below.

As a business, we need to ensure that our computer systems and emails are not used inappropriately and that those working for the business are doing so efficiently and effectively. We do not routinely look at the contents of individual emails, but in the course of normal business we may monitor both the flow and the subject lines of emails. We will only read the content of emails where we need to do so for good business reasons: for example, in order to investigate misconduct allegations or grievances of any kind, for performance management purposes, to ensure the confidentiality of business or personal data, or where information needs to be extracted in your absence. Therefore, it is important that users bear in mind that their communications on work emails may not be entirely private and should certainly never use this medium for personal information that they wish to remain completely confidential.

Where we are looking at the content of emails which appear to be of a private nature, the partners will consider whether it is strictly necessary to do so for a specific purpose(s) in the interests of the business. This will be done on a case-by-case basis, and the partners will only give authority for this where they consider that the interests of the Firm outweigh those of the user and there is no viable alternative.

USE OF THE INTERNET AND INTRANET

Internet and intranet access is generally for business purposes. It is provided to enable better performance of an employee's duties. Unless there is an express business-related use for the material and the user has permission of [person], images or videos must not be downloaded.

We use independently supplied software and data to identify inappropriate or sexually explicit internet sites or emails. The Firm may block access from within the network to any websites which it considers to be inappropriate for users to access.

Anyone who uses the Firm's computer systems in an attempt to disable, defeat or circumvent any security facility designed to protect the Firm's computer systems will be the subject of disciplinary action, which may result in summary dismissal.

No user may use the Firm's computer or email facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

This policy and the firm's disciplinary procedure

A breach of any of the provisions of this policy or of the data protection policy will be treated as a disciplinary matter. In certain circumstances, a breach may amount to gross misconduct leading to summary dismissal.

Monitoring

Under the Regulation of Investigatory Powers Act 2000 and the Lawful Business Practice Regulations 2000, the Firm is entitled to monitor the use of the internet at work to check that they are business-related. These systems belong to the Firm and are connected to the outside telecommunications system.

The Firm monitors email traffic as set out above and we also look at the use of the internet (including sites visited) in order to ensure that all such systems are being used for legitimate business purposes and in order to monitor quality of service and effectiveness of training.

Compliance
Any incidents which may breach this policy will be dealt with promptly. A manager can request that a user's computer (including its storage devices) be investigated for evidence of a suspected breach of this policy.

SOCIAL MEDIA

This part of the policy sets out how users must behave when using the Firm's social media accounts. It also explains the rules about using personal social media accounts at work, and sets out rules and guidance about content. This part of the policy should be read in conjunction with the earlier section about internet use and the Firm's data protection policy, in particular the sections about commercially confidential information and data security.

These rules apply wherever the social media use takes place, and whether it is on the Firm's equipment or the user's personal device.

Social media sites and services include

- social networks eg Twitter and Facebook
- online review websites eg Trustpilot, TripAdvisor
- sharing and discussion sites eg Reddit
- photographic social networks eg Instagram
- professional social networks eg LinkedIn

The Firm recognises the increased use of social media by staff and others in the course of their private communication. [The Firm also uses and encourages harnessing social media in publicising the Firm's activities and building its profile, in marketing and in building relationships with current and potential clients.] While the Firm recognises the right of all users to access these media, they should never be used in such a way as to harm the Firm or to damage the user's relationship with colleagues or the wider world.

General principles

Users should bear in mind the general guidance set out below:

- **Ensure that you fully understand the social media platform that you are using**. Different platforms have differing rules about content, sharing of information and data protection.
- **Understand privacy settings**. It is vital that you know precisely with whom you are sharing your opinions or personal information. Generally it is unwise to post such matters without restriction on access.
- **Be polite and considerate.** You should use the same level of courtesy on a social media site that you would on an email. Intemperate, rude and abusive language is very unwise, and if the reader could establish a connection between your post and the Firm, we reserve the right to consider disciplinary action against you.
- **Think before you post.** Other people are not always reasonable in their behaviour and it is easy to get caught up in a dispute or argument. Ensure that you do not post something you might regret later by delaying before posting a response.
- **Be on your guard for security risks.** It is not uncommon for such platforms to be used by fraudsters, so always be careful to watch out for phishing, and for spam which might contain bugs, or hacking attempts.
- **Be very careful in linking yourself with the Firm.** Obviously where the social media activity is to further the Firm's business and in the course of your work, you will be speaking on our behalf, and the content should reflect this. However, you need to ensure that, when you are posting on private social media, you are mindful of whether a connection can be established between you and the Firm, and the content does not breach the rules laid out below.
- **Don't use social media to handle complex business matters.** Such channels may be a good way of a client alerting us to something, or to post an enquiry or a request for contact, but otherwise they should not be used for anything more complex.

Using social media within the business

Only those who have been authorised by [the Partners] to use social media accounts may do so. We only allow designated people to use these accounts in order to ensure that we present a consistent message to clients, prospective clients and to the wider world. No new accounts should be created without the permission of [the directors].

All postings to business social media accounts should be in line with the Firm's objectives. In particular they may be used to

- respond to client contact enquiries
- share blog posts, articles and other useful information for clients that we have created
- share articles, video, media and other content created by others which may assist clients
- provide followers with an insight into what is going on in the Firm eg new recruits, new offices or areas of business, charitable activities etc
- promote marketing campaigns
- support new services that we are providing for clients.

Users should be particularly careful when sharing content that is not created by the Firm. You should always read the whole content of any article or blog to ensure that you are happy with what it is saying; don't just post based on the headline.

Personal social media use

Personal social media accounts can be used to make professional contacts, to obtain content which helps with professional development and to build the business profile. Users must be aware of the following rules:

- Employees and others working for the Firm can use their personal social media accounts for work-related purposes during working hours, but this is only for a specific reason and should never affect their work, or prevent them from completing their allocated work tasks.
- Social media should never be used for personal reasons within work time and should be restricted to evenings and lunchbreaks.
- Employees and others should make it clear that their social media account does not represent the Firm's views or opinions, where it is obvious to readers that they work for the Firm, or the nature of the contacts means that the connection would be known to the reader.

Restrictions

In particular, users must not use social media, where it is the business account or a personal account which can be linked with the business, so as to

a) breach this policy
b) post messages, status updates or links to material or content that is inappropriate. Inappropriate content includes pornography or racial or racial slurs; gender-specific comments; information encouraging criminal activity or terrorism; or material relating to cults, illegal drugs or gambling. Inappropriate content also includes any text, images or other media which could reasonably offend someone on the basis of race, colour, sex, age, religious or political beliefs, national origin, disability, sexual orientation or any other characteristics protected by law.
c) breach the Firm's obligations to any regulatory bodies
d) breach any professional obligation of confidentiality
e) defame or disparage the Firm and/or those who work for us, clients, business partners, suppliers or other stakeholders
f) harass or bully their colleagues in any way
g) damage the reputation of the Firm by associating it with inappropriate content
h) breach any other legal or ethical standards
i) publish or share any copyrighted material, media or materials owned by third parties unless this is permitted by the owner
j) share links to illegal copies of music, films, games or other software.

Breaches of the policy

We take the misuse of social media very seriously. If users are found to be in breach of this policy, they are likely to be subject to disciplinary action, up to and including termination of employment or engagement with the Firm. Where appropriate, we may also involve the police or other law enforcement authorities.

I confirm that I have read and understood the contents of this computer use policy and agree to abide by the terms stated therein. I consent to the Firm monitoring and intercepting incoming/outgoing email, voicemail and internet use for legitimate business reasons and to ensure that this policy is being adhered to. I agree that the Firm may inspect its computer equipment supplied to me or in my possession or control in the event it is suspected by management that I have breached the terms of this policy.

Signed:.....Date:.....

Please print name .....